

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-265581

(43)Date of publication of application : 28.09.2001

(51)Int.Cl.

G06F 9/06

H04L 9/32

(21)Application number : 2000-078395

(71)Applicant : CANON INC

(22)Date of filing : 21.03.2000

(72)Inventor : KIYOUTOKU SATOSHI

(54) SYSTEM AND METHOD FOR PREVENTING ILLEGAL USE OF SOFTWARE

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the illegal use of software.

SOLUTION: Key information concerning device ID characteristic to a device, which is recorded in a part of the device, is read and the device ID is collated with the device ID of a using-licensed device embedded in the software code of the software. Based on this collating result, the propriety of using the software is judged.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-265581
(P2001-265581A)

(43) 公開日 平成13年9月28日 (2001.9.28)

| (51) Int.Cl. ⁷ | 識別記号 | F I | タームコード (参考) |
|---------------------------|-------|--------------|--|
| G 0 6 F 9/06 | 5 5 0 | G 0 6 F 9/06 | 5 5 0 H 5 B 0 7 6 5 5 0 L 5 J 1 0 4 |
| H 0 4 L 9/32 | | H 0 4 L 9/00 | 6 7 3 B 6 7 5 D |

審査請求 未請求 請求項の数17 O L (全 7 頁)

(21) 出願番号 特願2000-78395(P2000-78395)

(22) 出願日 平成12年3月21日 (2000.3.21)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 京施 倫

東京都大田区下丸子3丁目30番2号キヤノン株式会社内

(74) 代理人 100086287

弁理士 伊東 哲也 (外1名)

Fターム(参考) 5B06 FB06 FB11 FB18

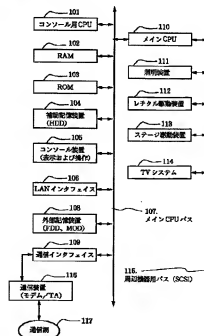
5J104 AAD7 AA12 KAO2 KAD4 KA14
NAD2 NA21

(54) 【発明の名称】 ソフトウェアの不正使用防止システムおよび不正使用防止方法

(57) 【要約】

【課題】 ソフトウェアの不正使用を防止する。

【解決手段】 装置の一部に記録した装置固有の装置IDに関する鍵情報を読み取り、装置IDとソフトウェアのソフトウェアコードに埋め込んだ使用許諾装置の装置IDとを照合し、この照合結果に基づいてソフトウェアの使用の可否を判断する。



【特許請求の範囲】

【請求項 1】 ソフトウェアおよびこのソフトウェアを使用する装置を含むソフトウェアの不正使用防止システムにおいて、前記装置を構成する部材または前記装置に付属する部材に記録した装置固有の装置 ID に関する鍵情報を読み取る手段、および前記装置 ID と前記ソフトウェアのソフトウェアコードに埋め込んだ使用許諾装置の装置 ID とを照合し、この照合結果に基づいて前記ソフトウェアの使用の可否を判断する手段を有することを特徴とする不正使用防止システム。

【請求項 2】 使用期限を定めた評価版のソフトウェアおよびこのソフトウェアを使用する装置を含む、ソフトウェアの不正使用防止システムにおいて、前記装置を構成する部材または前記装置に付属する部材に記録した前記ソフトウェアの使用期限に関する鍵情報を読み取る手段、および前記使用期限が現在の時刻を越えているか否かを照合し、この照合結果に基づいて前記ソフトウェアの使用の可否を判断する手段を有することを特徴とする不正使用防止システム。

【請求項 3】 ライセンス管理サーバー、前記ライセンス管理サーバーに第 1 の通信手段を介して接続される装置および前記装置で使用するソフトウェアを含む、ソフトウェアの不正使用防止システムにおいて、前記装置を構成する部材または前記装置に付属する部材に記録した装置固有の装置 ID または使用期限に関する鍵情報を読み取る手段、および前記ライセンス管理サーバー上で前記鍵情報を照合するために読み取った鍵情報を前記第 1 の通信手段により前記ライセンス管理サーバーへ定期的に伝達する手段を有することを特徴とするソフトウェアの不正使用防止システム。

【請求項 4】 前記鍵情報の照合を前記ソフトウェアによる処理の実行中に複数回行う手段を有することを特徴とする請求項 1、2 または 3 に記載の不正使用防止システム。

【請求項 5】 前記装置が第 2 の通信手段により複数接続される場合に、前記読み取った鍵情報を前記第 2 の通信手段を用いて他の装置へ伝達する手段を有することを特徴とする請求項 1～4 に記載のソフトウェアの不正使用防止システム。

【請求項 6】 前記装置が光学的に対象を認識可能な光学手段を有し、この光学手段を用いて前記鍵情報を読み取るものであることを特徴とする請求項 1～5 に記載の不正使用防止システム。

【請求項 7】 前記装置がレチクル上のパターンを投影レンズを介してウェハに露光するための露光装置であり、前記露光手段が前記レチクルまたはウェハを位置合わせするために前記レチクルまたはウェハ上の基準マークを撮像するものであることを特徴とする請求項 6 に記載の不正使用防止システム。

【請求項 8】 前記鍵情報を記録する部材が、半導体露光装置を構成する光学系部品であることを特徴とする請求項 6 に記載のソフトウェアの不正使用防止システム。

【請求項 9】 前記鍵情報を記録する部材が、半導体露光装置を構成するレチクルであることを特徴とする請求項 8 に記載のソフトウェアの不正使用防止システム。

【請求項 10】 前記鍵情報を記録する部材が、半導体露光装置を構成するレンズであることを特徴とする請求項 8 に記載のソフトウェアの不正使用防止システム。

【請求項 11】 前記鍵情報を記録する部材が、半導体露光装置を構成するウェハであることを特徴とする請求項 8 に記載のソフトウェアの不正使用防止システム。

【請求項 12】 前記鍵情報を記録する部材が、半導体露光装置を構成するステージであることを特徴とする請求項 8 に記載のソフトウェアの不正使用防止システム。

【請求項 13】 前記鍵情報を記録する部材が、半導体露光装置を構成するレチクル基準マークであることを特徴とする請求項 8 に記載のソフトウェアの不正使用防止システム。

【請求項 14】 前記鍵情報は、前記装置 ID もしくは前記使用期限を暗号化した情報または該暗号化した情報を復号するための鍵となる情報であることを特徴とする請求項 1～12 に記載のソフトウェアの不正使用防止システム。

【請求項 15】 ソフトウェアを使用する装置での前記ソフトウェアの不正使用を防止する方法において、前記装置を構成する部材または前記装置に付属する部材に記録した装置固有の装置 ID に関する鍵情報を読み取り、前記装置 ID と前記ソフトウェアのソフトウェアコードに埋め込んだ使用許諾装置の装置 ID とを照合し、この照合結果に基づいて前記ソフトウェアの使用の可否を判断することを特徴とする不正使用防止方法。

【請求項 16】 使用期限を定めた評価版のソフトウェアを使用する装置での前記ソフトウェアの不正使用を防止する方法において、

前記装置を構成する部材または前記装置に付属する部材に記録した前記ソフトウェアの使用期限に関する鍵情報を読み取り、前記使用期限が現在の時刻を越えているか否かを照合し、この照合結果に基づいて前記ソフトウェアの使用の可否を判断することを特徴とする不正使用防止方法。

【請求項 17】 ライセンス管理サーバーに接続される装置で使用するソフトウェアの不正使用を防止する方法において、

前記装置を構成する部材または前記装置に付属する部材に記録した装置固有の装置 ID または使用期限に関する鍵情報を読み取り、前記ライセンス管理サーバー上で前記鍵情報を照合するために読み取った鍵情報を前記ライセンス管理サーバーへ定期的に伝達することを特徴とするソフトウェアの不正使用防止方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、半導体製造工場において使用されている特殊な光学系部品を有する半導体露光装置に適用されている高価なソフトウェアプログラム等のソフトウェアの不正使用防止方法およびソフトウェアの不正使用防止システムに関するものである。

【0002】

【従来の技術】近年、一般のパーソナルコンピュータはもちろんのこと、特定業務向けの装置（半導体製造装置等の機器制御プログラム、あるいはモバイル端末のようなものも）がフラッシュROM化されることによって機能のソフトウェア化が進み、機能の全部または一部をソフトウェアのみの更新で提供できるようになってきている。ユーザーは、ハードウェアの買い換えなしに、ソフトウェアを購入するだけで新しい機能を利用することができるのが一般的になってきている。

【0003】

【発明が解決しようとする課題】ところが、ユーザーの中には、新機能をもったソフトウェアを1パッケージだけ購入し、数十台の半導体露光装置等の装置に新機能をもったソフトウェアを違法コピーしてインストールし、利用してしまうという不正使用の問題が発生していた。

【0004】半導体製造関連のソフトウェアは、出荷本数が全世界で数本だけの場合もあるが、通常、莫大な開発費がかかるため、ソフトウェアの単価も数千円を越えることが多くある。このような高価なソフトウェアを違法コピーにより不正利用されてしまえば、開発費の回収が不可能となるため、抜本的な対策が必要とされていた。

【0005】従来、ソフトウェアの不正使用の防止方法としては、例えばソフトウェア供給媒体に特殊なノイズを記録してマスター媒体からのコピーを防止したり、ハードウェアにシリアル番号識別子（シリアルID）を持つ部品を取り付け、前記ハードウェアを識別することでソフトウェアの動作するハードウェア本体を限定したり、あるいはハードウェア本体のプリンタポート等の外部デバイス用インタフェースにハードウェア的な鍵（ハードウェアキー）を取り付けて、前記ハードウェアキーと通信できなければソフトウェアを動作させない等といった対策がとられていた。しかしながら、これらのソフトウェアの不正使用防止対策（プロテクト方法）は半導体製造工場等においているマニア技術者の手によって簡単にノンプロテクト化されているのが実状であった。

【0006】また一方、高価格ソフトウェアであるが故に、ユーザは購入前に一定期間の評価期間を設けて、評価版ソフトウェアを要求する場合がある。ソフトウェア供給メーカーでは、使用期限をソフトウェアのバイナリプログラム内に設定し、装置の時刻が評価期間を越えて

いれど動作させないようにして評価版ソフトウェアを供給していた。ところが、ユーザの中には故意に装置の時刻を過去に戻し、継続的に高価格ソフトウェアを不正使用する例が多々発生していた。

【0007】本発明の第1の目的は、特殊な光学部品を用いたライセンスキーの偽造されにくい性質を利用して違法コピーによるソフトウェアの不正使用を防止することにある。

【0008】本発明の第2の目的は、評価版ソフトウェアの評価期間を越えて不正使用することを防止することにある。

【0009】本発明の第3の目的は、ハッキング等により本発明のプロテクト方法が破られた場合に、不正使用をライセンス管理元で察知し、ライセンス使用元への警告・訴訟のためのデータを取得できるようにすることである。

【0010】本発明の第4の目的は、ソフトウェアプログラム実行中に何度も照合を行うことで不正使用防止のレベルを向上することにある。

【0011】本発明の第5の目的は、ネットワークを介して装置固有のIDを通信することにより、装置IDが記録された特殊な光学系部品によるライセンスキーの供給数を最小限にすることにある。

【0012】

【課題を解決するための手段および作用】上記目的を達成するため、本発明は、以下のような構成を有する。すなわち、本発明の第1の構成は、ソフトウェアおよびそのソフトウェアを使用する装置を含む、ソフトウェアの不正使用防止システムまたは不正使用防止方法において、装置を構成する部材または装置に付属する部材（例えば、半導体露光装置等に使用される特殊な光学系部品であるレチクル、レンズ、ウエハ、ステージ、レチクル基準マーク等）に記録した装置固有の装置IDに関する鍵情報を、ソフトウェアプログラムの実行前あるいは実行中等に読み取り、読み取った装置IDとソフトウェアのコードに埋め込んだ使用許諾装置の装置IDとを照合し、この照合結果に基づいてソフトウェアの使用の可否を判断することを特徴とする。

【0013】ここで、装置固有の装置IDとプログラム動作許諾装置IDが相違していた場合には、前記装置制御ソフトウェアを動作不可能とする手段により、半導体製造工場等で横行している違法コピーによるソフトウェアの不正使用を防止するという作用がある。また、本発明は、レチクル、レンズ、ウエハ、ステージ等の特殊な光学系部品にソフトウェア使用権に関する情報を記録した場合、偽造が格段に難しくなることから、高価なソフトウェアが使用される半導体露光装置等には特に有益である。

【0014】本発明の第2の構成は、使用期限を定めた評価版のソフトウェアおよびそのソフトウェアを使用す

る装置を含む、ソフトウェアの不正使用防止システムまたは不正使用防止方法において、特殊な光学部品等に記録されたソフトウェアの使用期限に関する鍵情報を読み取る手段、および使用期限が、装置の時刻情報等から参照した現在の時刻を越えているか否かを比較照合し、この照合結果に基づいてソフトウェアの使用の可否を判断する手段を有することを特徴とする。

【00105】この構成によれば、使用期限が、現在の時刻を越えていた場合にはソフトウェアの動作を停止する手段を設けることができるため、使用期限を越えた評価版ソフトウェアの使用を防止するという作用がある。また、鍵情報を記録した特殊な光学部品キーを貸出し、回収することで、装置の時刻を戻す等の不正使用を防止することができる。

【00106】本発明の第3の構成は、ライセンス管理サーバ、ライセンス管理サーバに第1の通信手段を介して接続される装置およびこの装置で使用するソフトウェアを含む、ソフトウェアの不正使用防止システムまたは不正使用防止方法において、特殊な光学部品等に記録された装置固有の装置IDまたは使用期限等に関する鍵情報を読み取る手段、およびライセンス管理サーバ上で照合するために読み取った鍵情報等を、ネットワーク通信技術等を用いた第1の通信手段（例えば、インターネット）によりライセンス管理サーバへ定期的に通知する手段を有することを特徴とする。

【00107】そして、ライセンス管理元で管理している装置ID情報の重複および偽造等のライセンス違反を検出する手段を設け、ライセンス使用元でソフトウェアの不正使用の防止およびライセンス違反に対する警告・訴訟のための証拠データを取得できる。

【00108】本発明の第4の構成は、ソフトウェアによる処理の実行中に一定の基準で随時何度でも鍵情報の読み取りおよび照合を行う手段を有することを特徴とする。

【00109】この構成により、上述の構成により得られるセキュリティレベルを更に向上させることができる。

【00200】本発明の第5の構成は、装置がネットワーク通信技術等を用いた第2の通信手段（例えば、LAN）により複数接続される場合に、読み取った鍵情報等を第2の通信手段を用いて他の装置へ伝送する手段を有することを特徴とする。

【00201】これにより、ネットワーク上の他の装置に、ソフトウェア使用権をもつ装置の存在を常時に渡って通知する手段を設ければ、鍵情報の記録された特殊な光学部品キーをもたない装置に対してもソフトウェア使用権を使用許諾数分だけ供与することが可能となるため、光学部品キーの作製を最小限に抑えることができる。

【00202】また、本発明における鍵情報とは、装置の製造シリアル番号やソフトウェアの使用期限等をそのまま平文で記録したものであっても、これらを暗号化した

情報または暗号化した情報を復号するための鍵となる情報であってもよい。この場合は、例えば、装置を構成する部材の一部に暗号化した情報を記録し、他の一部または他の部材の一部に復号するための鍵となる情報を記録することにより、セキュリティレベルを更に向上させることができる。

【00203】

【実施例】（第1の実施例）本実施例では、高額のソフトウェアが搭載される装置の例として、ステップ等の半導体露光装置に本発明を適用した場合を説明する。図1は、本実施例における半導体露光装置のハードウェアシステム構成を説明するブロック図である。図1において、101はコンソール用CPUであり、半導体露光装置のコンソール表示とコンソールコマンド入力による操作の制御を司る。102はCPU101が実行プログラムを格納したりデータを格納するためのRAM、103はプログラムを格納するためのROM、104はデータおよびプログラムを格納するために用いられる補助記憶装置（ハードディスク等）である。本発明でソフトウェアの不正使用から保護されるべき高価格ソフトウェアプログラムは、補助記憶装置104上に保存される。ソフトウェアプログラムは、一般にファイルシステムを補助記憶装置104上に構成しファイルとして管理する。補助記憶装置104には一般にハードディスク等の磁気ディスク装置（HDD等）を用いることが多いが、装置の構成や露光作業の性質、運用の違いによって、フラッシュメモリやNVRAM（不揮発性メモリ）、EEPROM（電気消去可能プログラマブルROM）といったソフトウェア的な書き換えが可能な部品を用いる場合もある。105はコンソール装置でありオペレータ（操作者）は本装置よりコンソール用CPU101に対する指令を行うことができる。コンソール装置105の表示装置としては、CRTや液晶表示装置、ELパネル、あるいはプラズマディスプレイなどが一般的に用いられる。またコンソール装置105の入力装置としてはコマンドをキー入力するためのキーボードが用いられることが多いが、電子ペンによるペン入力装置（タブレット）やタッチパネルなどで構成されることもある。

【00204】106は、LANインタフェースであり、LANを介して他の半導体製造装置やサーバとデータの送受信を行う。LANの方式には、一般にTCP/IP等の方式が用いられるが、各ベンダーによって開発されたLAN方式のうち、どのようなものを採用しても構わない。108は外部記憶装置である。外部記憶装置108としてはFDD（フロッピーディスクドライブ）やMOD（光磁気ディスクドライブ）といったものが考えられる。本発明でソフトウェアの不正使用から保護される高価格ソフトウェアプログラムは一般に前記外部記憶装置108からソフトウェアのみの形態でFDやMOといった供給媒体に保存されて供給されることが多いが、

ネットワークインストール等ができる場合は外部記憶装置108は必須ではない。前記ネットワークインストール等を採用する場合は、LANインタフェイス106等を装備する必要がある。ネットワークインストール等を採用する場合であっても、ソフトウェアのインストール基本動作としては全く同一でよい。本実施例ではネットワークインストールを用いた実施例の詳細は説明しない。109は、通信装置(モデム/TA)116と通信を行うための通信インタフェイスである。通信インタフェイス109は一般にRS232C等のシリアル通信インタフェイスを用いる場合が多いが、通信におけるデータ量によってはパラレルインタフェイスやUSBインタフェイス等を用いても構わない。通信インタフェイス109と通信装置(モデム/TA)116の間で通信を行う場合のプロトコルは無手順非同期方式が一般に用いられるが、同期式やバタリ手順を採用しても構わない。110は、半導体露光装置を構成する各種の制御装置を全体制御するメインCPUである。メインCPU110とコンソール用CPU101はメインCPUバス107によって接続されて半導体露光装置として動作する。111は、半導体製造用のウェハに対して露光するための光源を制御する照明装置、112は半導体製造用のウェハに対して露光するパターンを描いたレチクル(フォトマスク)の搬入搬出等を制御するためのレチクル駆動装置、113は半導体製造用のウェハをステップアンドリビートの方式で露光するためにXYステージ上などでウェハを駆動制御するためのステージ駆動装置、114は半導体製造用のウェハを正確な位置決めをして制御するためのアライメント用TVシステムである。これら111、112、113、114の各装置は、周辺機器用バス115によりメインCPU110の制御下におかれる。周辺機器用バス115は、本実施例ではSCSIを用いているが、どのような汎用の標準バスで構成されていても構わない。

【0025】図2は、本実施例に係る半導体露光装置の模式図である。図2において、201は露光光源即ち照明装置、202は露光量制御のためのシャッタ、203は回路パターンの原板となるレチクル、204はレチクル203を保持するためのレチクルステージ、205はレチクル203を搬入するためのレチクルハンド、206は投影レンズ、207は半導体基板であるウェハ、208はウェハ207を保持し露光光源とのフォーカスを合わせるためのウェハZステージ、209はウェハZステージ208をXY方向へ移動させるためのXYステージ、210はXYステージ209の位置を計測するためのレーザ干渉計、211は露光処理をするためのウェハ207をウェハZステージ208へ供給するためのウェハ供給ハンド、212は露光処理を終えたウェハ207をウェハZステージ208から回収するためのウェハ回収ハンドである。

【0026】図2に示した半導体露光装置等の光学機器には、レチクル203やレチクルステージ204、あるいはウェハステージ208および209といった特殊な部品を具備している。レチクル203やその他のステージ等には、レチクル203やウェハ207の位置合わせを行うためのレチクルセットマークやレチクル基準マーク、ステージ基準マーク、TTL-AF基準マークあるいはウェハ基準マークといったマイクロメータ単位の微小なパターンマーク図形(不図示)が書き込まれており、前記パターンやマークの読みとりには微小パターンを読みとるための各種の特殊な光学系スコープ(不図示)を用いる。本実施例では、前記パターンやマークとして、装置固有のIDをテストレチクルやテストウェハ、あるいは半永久的に交換する可能性のないステージ等に微小パターンとして書き込み、前記装置IDを前記光学系スコープにより読みとる手段を具備することによって装置IDを生成する。装置IDとして特殊な光学系デバイスと光学系システムとを必要とし、かつ前記装置IDの読みとり手段を少なくとも1回以上必ず実行しなければ装置IDを取得できない構成となるため、装置IDの偽造や改ざん、あるいは装置IDの読みとり手段のバイパスによる不正使用に対して強力な防衛手段となる。レチクル203等の光学部品に書き込まれた文字パターン等のデータは、前記光学系スコープにより読みとったデジタル画像から文字認識を行い、文字データとして取得するのが望ましい。前記文字データは、装置の製造シリアル番号等をそのままASCIIコード等で記述したものを装置IDとして利用してもよいが、装置の製造シリアル番号等を秘密鍵によって暗号化した文字データをレチクル203等の特殊光学部品に書き込み、前記暗号化された装置IDの復号は、装置中の別の特殊光学部品、例えばレチクルステージ204に記録された秘密鍵を用いて復号し、ソフトウェアの使用を許可されている装置IDとの照合を行う構成とすることで、より強力な防衛手段となる。

【0027】図3は、本発明の第1の構成の一実施例に係るソフトウェアの動作を示すフローチャートである。以下、図3のフローチャートに沿って、本ソフトウェアの動作を説明する。ソフトウェアプログラム中にはあらかじめ、図3に示した本発明のフローチャートを実行するルーチンが、数力所から場合によっては数百箇所に通ってソフトウェアプログラム作成時に埋め込まれる。ソフトウェアプログラムの動作がソフトウェア使用許諾のチェック部分に分歧して実行されると、ステップ301からの一連の手順を実行することとなる。

【0028】まず、ステップ301で、装置に使われているレチクル等の特殊な光学系部品に書き込まれた装置固有の装置IDを取得する。次にステップ302で、装置上のRAM102上に取得した前記装置IDを記憶する。

【0029】次にステップ303で、ソフトウェアプログラム内に記憶されている使用許諾装置IDの読み出しを行う。次にステップ304で、装置上のRAM102上に取得した装置IDと使用許諾装置IDを比較し、これらが合致した場合はプログラムの実行を継続する。装置IDに相違がある場合は、ステップ305にすすみ、ソフトウェア使用者への警告、すなわち警告メッセージの表示等を行って、プログラムの実行を終了し装置の動作を停止する。

【0030】本発明のこのような動作により、ユーザが使用許諾のない装置に対してソフトウェアプログラムをインストールした場合に、ソフトウェアの不正使用を防止することができる。

【0031】(第2の実施例) 第1の実施例において、図3のフローチャートに示した処理を、タイマー動作等により一定の基準で随時何度も照合を行うようにする。本実施例のこのような動作により、ソフトウェア起動時のみに本発明のソフトウェアプロテクト手法を施されたとしても、装置動作中に何度も使用許諾のチェックを行うことにより、セキュリティレベルの向上が図られる。

【0032】(第3の実施例) 本実施例では、使用される特殊な光学部品に記録される情報として、評価版ソフトウェアの使用期限を記録することにより、評価版ソフトウェアの不正継続使用を防止することができる。ソフトウェアプログラムのコンパイルリンク時に、ソフトウェアを評価使用できる使用期限をプログラムのバイナリコード内に数カ所から数百箇所にかけて埋め込んでおく。ユーザには、使用期限のあるソフトウェアプログラムが記録された媒体とともに、ライセンスキーとなる光学部品、例えばキーとなるレチクル等を読み出す。ライセンスキーとなる光学部品に書かれた使用期限を経過した場合、あるいはライセンスキーとなる光学部品が存在しない場合には、評価版ソフトウェアを実行することができない。本実施例のこのような動作により、ユーザの評価版ソフトウェアの不正継続使用を防止することができる。

【0033】(第4の実施例) 本発明を実施する装置が、LAN等のネットワーク通信技術を用いて相互に接続されている場合、特殊な光学部品に記録された装置ID情報を装置IDと使用許諾するライセンス数が記録された装置IDと使用許諾するライセンス数が記録されたライセンスキーとなる光学部品を互ひつだけライセンス使用先に供給するだけで不正使用防止とソフトウェアの使用権付与が可能となる。

【0034】(第5の実施例) 第1、第2、第3または第4の実施例において、もしも何らかの手段により光学部品に書き込まれた装置IDの複製、あるいはRAM102上の装置IDの改ざん、あるいは、装置ID照合手順のバイパス等によって、本方式のプロテクトが破られ

た場合に、ライセンス管理元で前記プロテクト破りが発生したことを検知するため、特殊な光学部品から取得した装置IDデータを、インターネット等の通信手段を用いてライセンス管理元へ通知し、装置IDの複製・重複・照合手順のバイパス等が行われているのを検知してプロテクト破りを発見し、警告および告発のための証拠とする。

【0035】

【発明の効果】以上説明したように、本発明の第1の構成によれば、特殊な光学部品を用いたライセンスキーの偽造がされにくい性質を利用し、使用許諾された装置IDを取得できない場合、または装置IDの相違がある場合に、ソフトウェアプログラムを動作不可能として不正使用を防止し、適正な利潤を得ることができるという効果がある。

【0036】本発明の第2の構成によれば、評価版ソフトウェアの評価期間を超えて不正使用することを防止することができるという効果がある。

【0037】本発明の第3の構成によれば、本発明のプロテクトが破られた場合に、プロテクト破りがなされたことを検知し、ライセンス違反の警告・告発のための情報を取得して、裁判等を有利に進めるための証拠とすることができるという効果がある。

【0038】本発明の第4の構成によれば、ソフトウェアプログラム実行中に何度も装置IDの照合を行うことで不正使用防止のレベルを向上することができるという効果がある。

【0039】本発明の第5の構成によれば、ネットワークを介して装置固有のIDを通信することにより、装置IDが記録された特殊な光学系部品によるライセンスキーの供給数を最小限にすることができるという効果がある。

【図面の簡単な説明】

【図1】 本発明に係る半導体露光装置のハードウェア構成図である。

【図2】 本発明に係る半導体露光装置の模式図である。

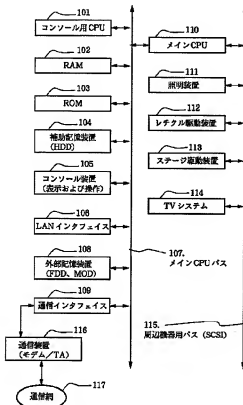
【図3】 本発明の第1の実施例の動作を説明するフローチャートである。

【符号の説明】

101: コンソール用CPU、102: プログラムを格納したりデータを格納するためのRAM、103: プログラムを格納するためのROM、104: データおよびプログラムを格納するための補助記憶装置、105: コンソール装置、106: LANインタフェース、107: メインCPUバス、108: 外部記憶装置、109: 通信インタフェース、110: メインCPU、111: 照明装置、112: レチクル駆動装置、113: ステージ駆動装置、114: アライメント用TVシステム、115: 周辺機器用バス、116: 通信装置 (モデ

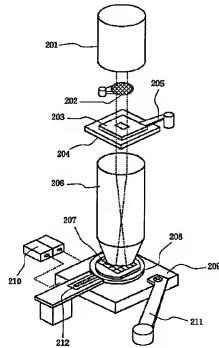
ム・TA)、117:通信網、201:露光光源(照明装置)、202:露光量制御用シャッタ、203:レチクル、204:レチクルステージ、205:レチクルハンド、206:投影レンズ、207:ウエハ、208:*

【図1】

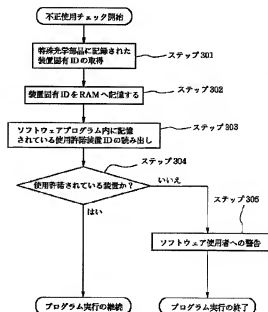


*ウエハZステージ、209:ウエハXYステージ、210:レーザ干渉計、211:ウエハ供給ハンド、212:ウエハ回収ハンド。

【図2】



【図3】



SPECIFICATION <EXCERPT>

[0026]

The optical apparatus such as the semiconductor exposure apparatus, as shown in FIG. 2, has special components, for example, a reticle 203 and a reticle stage 204, or wafer stages 208 and 209. A micrometer-size pattern mark (not shown), for example, a reticle setting mark, a reticle fiducial mark, a stage fiducial mark, a TTL-AF fiducial mark, or a wafer fiducial mark to align the reticle 203 and the wafer 207, is drawn on the reticle 203, the other stages, or the like, and thus various special optical scopes (not shown) for reading a minute pattern are used to read the pattern and mark. In this embodiment, an apparatus ID is generated by providing a unit for reading, with the optical scope, a unique ID for the apparatus drawn on a test reticle, a test wafer, a semi-permanent stage, or the like as the pattern and mark, i.e. the minute pattern. A special optical device and an optical reading unit are needed for the apparatus ID, and the apparatus is designed such that the apparatus ID cannot be obtained unless the reading unit for the apparatus ID is executed at least one or more times. Accordingly, this apparatus provides a robust security against abuse by counterfeiting or tampering of the apparatus ID, or bypassing the reading unit for the apparatus ID. Preferably, data drawn on the optical component such as the reticle 203, for example, a character pattern, is obtained as character data by performing a character recognition on the digital image. With respect to the character data, for example, the product serial number written in ASCII code may be used as the apparatus ID. However, this apparatus provides the more robust security by i) writing, on the special optical components, encrypted character data which is the product serial number encrypted with a private key, ii)

decoding the encrypted apparatus ID using the private key recorded on the other special optical component in the apparatus, for example, the reticle stage 204, and iii) matching the decoded apparatus ID with an apparatus ID authorized for the software.

[0033] (The fourth embodiment)

When the apparatus implementing the present invention is connected to the other apparatuses using the network communication technique such as LAN, the apparatus ID information recorded on the special optical component may be read through the LAN from only the licensed apparatuses. Such a relation structure can avoid the abuse and license the other apparatuses for the software just by providing, to the apparatuses to be licensed, only one optical component serving as a license key where the apparatus ID and the number of the license are recorded.